Brentwood Smith

From: Drake, Dan (USAGAS) <Dan.Drake2@usdoj.gov>
Sent: Wednesday, March 20, 2019 11:23 AM
To: Robert Balkcom; Capt. Billy Hitchens III; Dale E. Howell; Capt. Chad Riner; Chris Rodewolt
Subject: FW: Fort Stewart Weekly Security Report (19-12) (UNCLASSIFIED)
Attachments: 19-12 Fort Stewart Weekly Security Report (20 Mar 19).pdf; 19-12 Social Media and OPSEC.pdf; 19-12 Seven Step Plan For Writing Classification Guides.pdf; 19-12 Deep Web Ultimate Guide.pdf

CLASSIFICATION: UNCLASSIFIED

Good Morning. The Fort Stewart Weekly Security Report is a review of unclassified open source security related articles and is intended for security education purposes only. The report is not intended or implied to replace any official Department of Defense or U.S. Army intelligence reports. This report is provided for security managers and/or other security professionals to keep abreast of local, regional, and national security related circumstances, trends, new technologies and situational awareness.
To be added or removed from the Fort Stewart Weekly Security Report distribution list, just send an e-mail to leroy.h.malphrus.civ@mail.mil.
Thanks for your interest in the Fort Stewart Weekly Security Report.

LeRoy H. Malphrus Jr.
Chief, Security Division
1086 William H. Wilson Avenue
Bldg. 623, Suite 121
USAG Fort Stewart, GA 31314
Desk: (912) 767-1910/1891
DSN: 870-1910/1891
Cell: (912) 210-7208
Fax: (912) 767-2994

We are the Army's Home

CLASSIFICATION: UNCLASSIFIED

Directorate of Plans, Training Mobilization and Security
Security Division

Fort Stewart Weekly Security Report
2019 Edition

The Fort Stewart Weekly Security Report is a free unclassified open source document to support security education training awareness. The report is not intended or implied to replace any official Department of Defense or U.S. Army intelligence reports. This report is provided for security managers and/or other security personnel to keep abreast of local, regional, and national security related circumstances, trends, new technologies and situational awareness.

CURRENT DEPARTMENT OF STATE TRAVEL ALERTS AND WARNINGS

DEPARTMENT OF STATE TRAVEL ADVISORY LEVELS

Level 1 - Exercise Normal Precautions: This is the lowest advisory level for safety and security risk. There is some risk in any international travel. Conditions in other countries may differ from those in the United States and may change at any time.

Level 2 - Exercise Increased Caution: Be aware of heightened risks to safety and security. The Departments of State provides additional advice for travelers in these areas in the Travel Advisory. Conditions in any country may change at any time.

Level 3 - Reconsider Travel: Avoid travel due to serious risks to safety and security. The Department of State provides additional advice for travelers in these areas in the Travel Advisory Conditions in any country may change at any time.

Level 4 - Do Not Travel: This is the highest advisory level due to greater likelihood of life-threatening risks. During an emergency, the U.S. government may have very limited ability to provide assistance. The Department of State advises that U.S. citizens not travel to the country or to leave as soon as it is safe to do so. The Department of State provides additional advice for travelers in these areas in the Travel Advisory. Conditions in any country may change at any time.

[redacted]

[redacted]

[redacted]

TRAVEL ALERT/SITUATIONAL AWARENESS - MEXICO (SPRING BREAK): U.S. Embassy Mexico City warns, each year thousands of U.S. citizens visit Mexico during Spring Break (February, March and April). While the vast majority of travelers have safe and enjoyable trips, Spring Break travel can sometimes include unforeseen problems such as the following:

✓ **Medical Emergencies**: An illness or accident could result in the need to seek medical treatment or hospitalization in Mexico. Private hospital prices are comparable, and often higher, to those in the United States. Many facilities require payment either before providing treatment or before discharging a patient. Make sure your health insurance plan provides coverage overseas or purchase travel insurance that specifically covers you in Mexico. Seek coverage that includes medical evacuation. Confirm costs of medical treatment in advance, when possible.

- **Drowning**: Some beaches have strong undercurrents and rip tides. Beaches may lack lifeguards, warnings, or signs of unsafe conditions. Avoid strong currents and do not swim after drinking or when warning flags note unsafe conditions.

- **Unregulated Alcohol**: The legal drinking age in Mexico is 18. U.S. citizens have reported losing consciousness or becoming injured after consuming unregulated alcohol. Drink responsibly and watch your drink at all times. If you begin to feel ill, seek medical attention immediately. Report cases of unregulated alcohol to the Mexican Federal Commission for the Protection against Sanitary Risk (COFEPRIS) at contactociudadano@cofepris.gob.mx.

- **Sexual Assault**: Rape and sexual assault are serious problems in some resort areas. Many of these incidents occur at night or during the early morning hours, in hotel rooms, on deserted beaches, and may follow the drugging of drinks. Perpetrators may target inebriated or isolated individuals. Know your drinking companions and stay in a group of friends who have your safety in mind when you are in clubs and bars, out walking in dimly-lit areas, or in a taxi at night. Be aware of your safety and protect your personal possessions when using public transportation. Use radio taxis or those from “sitio” taxi stands. Obey Mexican law and remember Mexican laws may differ from U.S. laws. The phone number to report emergencies in Mexico is “911”: Although there may be English-speaking operators available, it is best to seek the assistance of a Spanish speaker to place the call.

- **Drugs**: Carrying any form of marijuana into Mexico, even with a prescription

or medical marijuana license, is a Mexican federal offense and considered as international drug trafficking. Offenders can expect large fines and/or jail sentences of up to 25 years. Mexican criminal organizations are engaged in a violent struggle to control trafficking routes. Criminal organizations have targeted unsuspecting individuals who regularly cross the border as a way to smuggle drugs into the United States. Frequent border crossers are advised to vary their routes and travel times, and to closely monitor their vehicles to avoid being targeted. U.S. citizens are advised to carry a copy of their prescription or doctor's letter, but it is still possible that they may be subject to arrest for arriving in Mexico with substances on these lists. Note that medicines considered "over the counter" in the United States may be a controlled substance in Mexico. For example, pseudoephedrine, the active ingredient in Sudafed, is considered a controlled substance in Mexico.

- **Guns and Ammunition**: Weapons laws in Mexico vary by state, but it is generally illegal for travelers to carry weapons of any kind including firearms, knives, daggers, brass knuckles, as well as ammunition (even used shells). Illegal firearms trafficking from the United States to Mexico is a major problem, and the Department of State warns all U.S. citizens against taking any firearm or ammunition into Mexico. If you are caught entering Mexico with firearms or ammunitions, you will be imprisoned.

- **Arrests**: Drunk and disorderly behavior and urinating in public are illegal in Mexico. If you break Mexican law, you can be arrested. Keep your friends and family back home informed of your travel plans, especially if traveling alone. If you are arrested or detained, ask police or prison officials to notify the U.S. Embassy or nearest U.S. Consulate immediately. The Mexican government is required by international law to contact the U.S. Embassy or consulate promptly when a U.S. citizen is arrested, if the arrestee so requests. This requirement does not apply to dual nationals. https://mx.usembassy.gov/security-alert-u-s-embassy-mexico-city/

SITUATIONAL AWARENESS - MEXICO (TIJUANA RANKS THE MOST VIOLENT CITY WORLDWIDE): The Citizen Council for Public Safety and Criminal Justice presented this on 12 March, its ranking of the 50 most violent cities worldwide, in which Tijuana was placed in the first place with 2,640 homicides registered during the past year. Within the first five places, three other Mexican cities follow the border municipality by its high rates of intentional homicides, which are Acapulco with 948, Ciudad Victoria with 314 and Ciudad Juarez with 1,251. This association has been carrying out this list since 2008, with which it measures the levels of violence that are lived around the world, in this year Mexico was placed as the country with the most cities mentioned, while Brazil, which had remained in the first place , went down to the second. The measurement in the number of murders committed per 100 thousand inhabitants, in his case Tijuana has 1,909,424 inhabitants, so it shows a rate of 138.26 homicides per 1,000 population. According to the information shared with the civil organization, it is the second consecutive year in which a Mexican city occupies the first place, the city of Los Cabos was in this position in 2017 with 365 homicides that for its population of 328,245 inhabitants resulted with a rate of

111.33 murders registered in 2017. In 2017, Tijuana ranked fifth. Other Mexican cities that appear in the 2018 list are Irapuato, Cancún, Culiacán, Uruapan, Ciudad Obregón, Coatzacoalcos, Celaya, Ensenada, Tepic, Reynosa and Chihuahua. http://www.borderlandbeat.com/2019/03/tijuana-ranks-most-violent-city.html

TRAVEL ALERT/SITUATIONAL AWARENESS - THE BAHAMAS: On 25 February 2019, the U.S. State Department has issued a travel warning to Americans visiting the Bahamas. Violent crime, such as burglaries, armed robberies, and sexual assault, is common, even during the day and in tourist areas. Anyone traveling to the islands should "exercise extreme caution," according to the warning. The Bahamas is considered a "Level 2" warning, along with Belize, which has similar crime warnings, and European countries such as Germany, Spain and France which face terrorism threats. Although the family islands are not crime-free, the vast majority of crime occurs on New Providence and Grand Bahama islands. U.S. government personnel are not permitted to visit the Sand Trap area in Nassau due to crime. Activities involving commercial recreational watercraft, including water tours, are not consistently regulated. Watercraft are often not maintained, and many companies do not have safety certifications to operate in The Bahamas. Jet-ski operators have been known to commit sexual assaults against tourists. As a result, U.S. government personnel are not permitted to use jet-ski rentals on New Providence and Paradise Islands. Tourists also may encounter drug or human smugglers who threaten them "in an attempt to coerce them into smuggling on their behalf," the warning said. They also might encounter credit card fraud, real estate scams or timeshare scams. https://www.newsmax.com/newsfront/bahamas-travel-warning/2019/03/02/id/905152/ and https://travel.state.gov/content/travel/en/international-travel/International-Travel-Country-Information-Pages/Bahamas.html

CIA WORLD FACTBOOK https://www.cia.gov/library/publications/the-world-factbook/

US CITIZENS WILL NEED TO REGISTER TO VISIT PARTS OF EUROPE STARTING IN 2021: US citizens visiting parts of Europe will need authorization from the European Union come 2021. The EU announced last year it was creating a European Travel Information and Authorization System, or ETIAS. That will require "pre-travel screening for security and migration risks of travelers benefiting from visa-free access to the Schengen area." The Schengen Area is a zone of 26 European countries that do not have internal borders and allow people to move between them freely, including countries such as Spain, France, Greece, Germany, Italy and Poland. Currently, US citizens can travel to Europe for up to 90 days without any sort of travel authorization. ETIAS will change that. Visa-free travelers, including US citizens, will need to request ETIAS authorization before visiting the Schengen Area. They can complete an application and pay a service fee of 7 euros (about $8) online. The authorization is valid for three years. "Completing the online application should not take more than 10 minutes with automatic approval being given in over 95% of cases," the European Commission said in a statement. The United States has a similar system called the Electronic System for Travel Authorization, or ESTA. "We

are aware of the European Union's plan to implement its own travel information and authorization system, similar to the U.S. ESTA, to contribute to a more efficient management of the EU's external borders and improve internal security," a US State Department official said in a statement. "Each country has the right to determine its standards for entry." The official added that the "ETIAS authorization is not a visa." The United States won't be the only country affected by the changes. From 2021, citizens from 60 countries will be required to apply for the ETIAS before entering the Schengen Area. Brazil, Canada, New Zealand, Singapore, Israel and Mauritius are among those countries. The European Parliament agreed to establish ETIAS in July. At the time, Dimitris Avramopoulos, the European commissioner for migration, home affairs and citizenship, indicated that the requirement was put in place for security reasons. "The new ETIAS will ensure that we no longer have an information gap on visa-free travelers," he said in a statement. "Anyone who poses a migratory or security risk will be identified before they even travel to EU borders." https://edition.cnn.com/travel/article/us-citizens-need-visas-to-visit-europe-in-2021/index.html

REGION SITUATIONAL AWARNESS (FL, GA, and SC)

GA - GEORGIA WOMAN ARRESTED FOR CONSPIRING TO PROVIDE MATERIAL SUPPORT TO ISIS: Kim Anh Vo, a.k.a. "F@ng," a.k.a. "SyxxZMC," a.k.a. "Zozo," a.k.a. "Miss.Bones," a.k.a. "Sage Pi," a.k.a. "Kitty Lee," was arrested on 12 March 2019 in Hephzibah, Georgia. Vo was charged by a criminal Complaint with conspiring to provide material support to the Islamic State of Iraq and al-Sham (ISIS), a designated foreign terrorist organization. In April 2016, Vo joined the United Cyber Caliphate (UCC), an online group that pledged allegiance to ISIS and committed to carrying out online attacks and cyber intrusions against Americans. Since that time, the UCC and its sub-groups have disseminated ISIS propaganda online, including "kill lists," which listed the names of individuals - for example, soldiers in the United States Armed Forces and members of the State Department - whom the group instructed their followers to kill. For example, on or about April 21, 2016, the UCC posted online the names, addresses, and other personal identifying information of approximately 3,602 individuals in the New York City area and included a message that stated: "List of most important citizens of #New York and #Brooklyn and some other cities . . . We Want them #Dead." Between April 2016 and May 2017, Vo worked on behalf of the UCC to recruit others to join the group and assist with the group's hacking efforts. Between January and February 2017, Vo recruited other individuals - including a minor residing in Norway - to create online content in support of ISIS, including a video (Video-1) threating a non-profit organization based in New York, New York, which was formed to find and combat the online promotion of extremist ideologies. Video-1 contained messages such as, "You messed with the Islamic State, SO EXPECT US SOON," followed by a scene displaying a photograph of the organization's chief executive officer and former U.S. Ambassador (CEO), along with the words: "[CEO], we will get you." On or about April 2, 2017, the UCC posted online a kill list containing the names and personal identifying information of over 8,000 individuals, along with a

links to another video (Video-2). Video-2 displayed messages stating, in part: "We have a message to the people of the U.S., and most importantly, your president Trump: Know that we continue to wage war against you, know that your counter attacks only makes stronger. The UCC will start a new step in this war against you. . . ." and "We will release a list with over 8000 names, addresses, and email addresses, of those who fight against the US. Or live amongst the kuffar. Kill them wherever you find them!" In subsequent scenes, Video-2 contains what appears to be a graphic depiction of the decapitation of a kneeling man. Vo, 20, of Georgia, is charged with one count of conspiring to provide material support to a designated foreign terrorist organization, which carries a maximum sentence of 20 years in prison. The maximum potential sentence in this case is prescribed by Congress and is provided here for informational purposes only, as any sentencing of the defendant will be determined by a judge. https://www.justice.gov/opa/pr/georgia-woman-arrested-conspiring-provide-material-support-isis

GA - $1.2M IN COCAINE, MARIJUANA SEIZED IN CHATHAM COUNTY: Two people were arrested after Chatham-Savannah Counter Narcotics agents seized $1.2 million worth of cocaine and $20,000 in cash from a semi-trailer in Chatham County. Husband and wife are charged with trafficking a controlled substance after agents found four kilograms of cocaine and more than 600 pounds of marijuana in the trailer, in addition to the money. "Really the best way to cripple organizations like this is to hit them where it hurts - take their large shipment of supply, take their money and arrest their more top-level players," said Gene Harley, assistant deputy director of the Chatham-Savannah Counter Narcotics Team. Harley says CNT's investigation started after a tip from the Pooler Police Department, and agents worked around the clock for about 48 hours to find the drugs. "We knew the drugs were here locally," he said. "It was finding them. It was almost playing an adult game of hide-and-seek, if you will, with drugs." He says the arrests and seizure are part of a larger investigation and show how traffickers are using Savannah's connectivity to get and send drugs throughout the southeast. "Drugs come in most of the time from outside the U.S.," Harley said. "They go to Atlanta, and from there, they're distributed throughout the entire southeast region. With Savannah only being a four-hour drive from there, you know, it plays a vital role into that. We're also finding more and more where Savannah is being recruited to be almost like a second tier to Florida. You take Atlanta, you hop down to Savannah, and from there; they feed into Florida." Harley said agents are also seeing more people from South Carolina coming into the area to buy large amounts of drugs to then sell elsewhere. Even with all of that movement, Harley said there's no question some of the drugs would've been sold and used in Chatham County if agents hadn't found them first. "The huge win for the community is this is obviously a very large amount of drugs we're talking about that would otherwise no doubt been distributed within Chatham and the surrounding counties, so they were here for the purpose of poisoning our community," Harley said. "Thankfully, we were successful in seizing them and getting them off the streets before they even had an opportunity to be distributed." Harley said the

investigation is ongoing, and he expects additional charges and more arrests in this case. http://www.wtoc.com/2019/03/12/m-cocaine-marijuana-seized-chatham-county/

GA - 260 ARRESTS MADE DURING SAVANNAH ST. PATRICK'S DAY FESTIVAL WEEKEND: The Chatham County Sheriff's Office has released a breakdown of arrests made in Chatham County throughout the St. Patrick's Day Festival Weekend. The Sheriff's Office says between Thursday, March 14 and Sunday, March 17, the Chatham County Sheriff's Office took in 260 arrested individuals into the Chatham County Detention Center. "This year's numbers were a little lower than last year," said Sheriff Wilcher. "I think we did about 325 last year, a normal weekend here at the jail Friday, Saturday and Sunday day and night, we normally do about 115 people, we did a survey from Thursday, Friday, Saturday and Sunday and up until midnight Sunday we took in 260 people." During a news conference Monday morning, city officials said workers and volunteers collected 183-tons of trash after thousands gathered in Savannah over the weekend for the St. Patrick's Day parade and festival. City officials say Savannah will be implementing some new rules throughout the parade area and enforcing those next year. One change that was mentioned would be to ban Styrofoam coolers from the parade route. http://www.wtoc.com/2019/03/18/ccso-arrests-made-chatham-county-during-st-patricks-day-weekend/

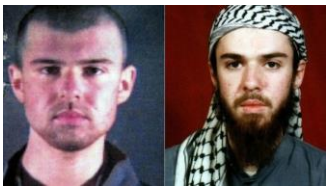
SC - 2 SOUTH CAROLINA MEN SENTENCED IN DARKNET MAIL BOMB CASE: Two men from South Carolina are currently serving sentences in federal prison after a court found them guilty of conspiring to murder the ex-wife of one of the defendants with a mail bomb. The two men are 32-year-old Michael Young Jr. and Tyrell Fears, who is Young's 23-year-old nephew. They are in the custody of the Broad River Correctional Institution in Columbia. Young was already in prison for a prior attempt to murder his ex-wife, Shauna Clark, and killing Robert Bell, her father. In 2007, he shot the woman and her father, who died attempting to protect her. The event took place at a parking lot in Columbiana Centre, a shopping mall. In 2011, the court sentenced Young to 50 years in prison. At the time, John Delgado, his defense attorney, stated that Young was remorseful and accepted responsibility for his actions. According to investigators, Young began shopping for explosives in February 2017. In prison, he used a contraband cellphone to access the dark web. Young then got in touch with a vendor on AlphaBay, a darknet market that was later seized by law enforcement in summer 2017. The user claimed to be a foreign distributor of explosives - a role used by a Federal Bureau of Investigation agent who was working undercover. The FBI agent identified himself as Marcus and specified that he was from Russia. Young and the agent communicated for months on the dark web before they agreed on how "Marcus" would deliver the explosive. Based on the prosecutors' report, Young paid the agent via Bitcoin to send a mail bomb to an accomplice's house. He further instructed the agent to send the reshipment label with his ex-wife's address to Volious' residence. The FBI created a fake bomb, in which they put some explosive residue that could explode without harming anyone. The

authorities delivered the bomb via mail. By this time, the FBI was monitoring Volious and Fears. There were 40 agents in several cars and two Cessna planes who were trailing them. Fears received the labels from Volious in June 2017. He placed the bomb inside the mail and delivered it to a post office. An inspector then went to the post office and intercepted the package. In April 2018, the court convicted Volious and Young for four offenses. The convictions included conspiracy, the transportation of an explosive with the intent to commit murder, sending a non-mailable explosive in the attempt to commit murder and transporting an explosive while committing another felony. The evidence that the authorities presented against Young indicated that his intent to murder his ex-wife was an obsession. Young's ex-wife had remarried and settled in Florida. Will Lewis, the assistant district attorney presenting this case, explained that the conspirators rigged the bomb so it could explode once the targeted victim opened the mail. Lewis recommended that the judge would give Young the maximum prison sentence, explaining that he acted cruelly and sadistically. Clark, Young's ex-wife, also presented her statement to the court saying that her children, always eager to open up packages, could have been killed in doing so. She also added that she suffers from the effects of psychological trauma involved with being the intended victim of a mail bomb. Young's prison term was set to 43 years, while Fears got 10 years after admitting that he carried an explosive while committing a felony. Young will begin serving his time after completing his 50-year sentence. The prosecutors stated that Volious' sentence for his participation in the plot would come later. District Court Judge Michelle Childs presided over the case. She stated that she made her ruling in consideration of the fact that Young appeared to be determined to murder his ex-wife, even though he was already in prison after the first attempt. Young told the judge that he was remorseful and took responsibility for his actions.
https://darkwebnews.com/law-enforcement/two-south-carolina-men-sentenced-in-darknet-mail-bomb-case/

SC - SC MAN SENTENCED TO 14 YEARS FOR ORDERING NARCOTICS FROM CHINA VIA THE DARK WEB: Terry Wooten, the chief U.S. District Judge of Columbia, South Carolina, has sentenced 37-year-old darknet drug dealer Eric Hughes to 168 months in federal prison. Hughes pleaded guilty last year to drug conspiracy and money laundering. He was arrested in August 2017 by a Drug Enforcement Administration-led task force, after he was involved in a car crash where the pills he was transporting were spilt on the roadway. Conferring on to local sources, Hughes and two of his co-defendants ran a pill manufacturing operation that sold counterfeit Oxycodone and Xanax prescription drugs. It is believed that drug users across the U.S. bought his pills from the dark web where he was identified under the moniker Genius Bar. Moreover, it is claimed that he has been overseeing the operation since 2012 and has sold millions of counterfeit pills to unsuspecting users as well as distributors. Evidence presented to the court show that Hughes bought a pill press to make his pills look similar to the real prescription pills. He outsourced his essential ingredients, alprazolam and synthetic opioid U-47700, from China using the dark web. Using the internet as his official guidebook, Hughes would mix the

ingredients, dye and a binding agent to produce approximately 4,500 pills an hour. The operation was carried out in clandestine pharmaceutical laboratories set up in rented vacation homes in Bluffton, Sullivans Island, Fripp Island, Isle of Palms and Tybee Island in Georgia. Hughes and his associates would use the houses for a month or so where it is believed approximately 500,000 counterfeit pills would be produced before they vacated. Revenue collected from the operation, predominately in Bitcoins, was laundered through various accounts to keep their source out of sight. In total, investigators seized around 150 Bitcoins worth $1 million, most of which were hidden in multiple places like gambling sites. Additionally, Hughes also gave family members Bitcoins worth $200,000. The U.S. Marshal's office has since auctioned the funds, but investigators believe that Hughes has more Bitcoins stashed away. Hughes has been in the Lexington County Jail after the judicial courts denied him bond. During the bond hearing, the prosecutor in charge of the case, Assistant U.S. Attorney Jim May, argued that he represented a threat to society and a flight risk. The assistant attorney cited reasons that during his arrest, he possessed a loaded pistol and fake identification as well as his stash of Bitcoins. Hughes is expected to cover the cost of cleaning up the contamination left by the clandestine laboratories. Through his testimony, Richland County Sheriff's Deputy William Cobia stated that owners of a house in Tybee Island spent $213,000 cleaning the contamination. The other two his alleged co-defendants, Willie Rice, 37, and Taylor Place, 25, are also expected to plead guilty to the same charges. If found guilty they both face 20 years in a federal prison with no parole. https://darkwebnews.com/law-enforcement/14yrs-sentence-for-ordering-narcotics-via-darknet/

SECURITY NEWS

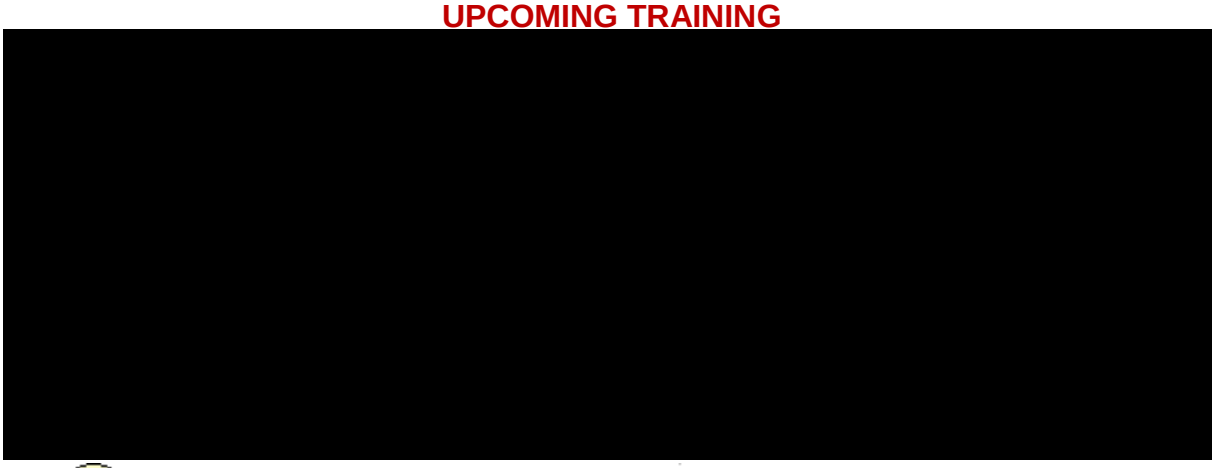


JOHN WALKER LINDH, AMERICAN EX-TALIBAN FIGHTER, TO BE RELEASED IN MAY, HASN'T DENOUNCED ISLAMISM: John Walker Lindh, a former American Taliban militant convicted in 2002 for supporting the terrorist organization, is due to be freed in May. The former Islamist fighter, dubbed "Detainee 001 in the war on terror," was arrested in 2001, just months after the Sept. 11 attacks and the start of the war in Afghanistan. Then just 20 years old, he was among a group of Taliban fighters who were captured by U.S. forces. Within a year, Walker Lindh was convicted of supporting the Taliban and sentenced to 20 years in prison -- even as some hardliners urged authorities to consider treason charges that could have resulted in the death penalty. Walker Lindh's release later this year is likely to be met with headaches for security services across the globe, especially since he has since acquired Irish citizenship and plans to move there -- even though he hasn't denounced radical Islamic ideology and has even made pro-Isis comments to the media. The National Counterterrorism Center penned a document dated Jan. 24, 2017 claiming the former Taliban fighter remains as radicalized now as he was in 2001. "As of May 2016, John Walker Lindh (USPER) - who is scheduled to be released in May 2019 after being convicted of supporting the Taliban - continued to advocate for global jihad and to write and translate violent extremist texts," the Foreign Policy

magazine reported. The report added Walker Lindh told “a television news producer that he would continue to spread violent extremist Islam upon his release.” It appears, however, that the Irish government won’t follow the example of the British government -- which rescinded a Jihadi bride’s British citizenship -- and won’t stop Walker Lindh from entering the country. “Irish citizens are not subject to immigration control,” the spokesman for Ireland’s Department of Justice told the London Times. “Therefore, if a person has Irish citizenship and presents their Irish passport on arrival, they will not be refused entry to the state.” Walker Lindh confirmed his plans to head to Ireland after his release in remarks he made to CAGE, a London-based organization focused on supporting people impacted by the War on Terror. “I don’t really know what to expect from the Irish government,” he wrote to the group, according to the newspaper. “I know virtually nothing about them. I think the only reasonable way to present my case to them is to explain my unique circumstances that make my survival in the US practically impossible." He added: “Essentially I am seeking asylum from one country where I am a citizen in another country where I am also a citizen. The worst they can do is decline my request. I figure it is worth at least trying.” In the U.S., meanwhile, multiple lawmakers have called for the creation of a registry of convicted terrorists, modeled after sex-offender registries, as multiple high-profile releases are set to take place in the next two years. https://www.foxnews.com/us/american-ex-taliban-fighter-to-be-released-in-may-seek-to-move-to-ireland-despite-authorities-warning-he-hasnt-denounced-islamism

[redacted]

UPCOMING TRAINING



DID YOU KNOW…IS ERIC ROBERT RUDOLPH DEAD OR STILL ALIVE? Eric Rudolph is still alive. He is currently 52 years old. Also known as the Olympic Park Bomber, Rudolph is a convicted American domestic terrorist for a series of anti-abortion and anti-gay-motivated bombings across the southern United States between 1996 and 1998, which killed two people and injured over 120 others. Rudolph served in the US Army from 1987-1989, but was discharged for smoking marijuana. Rudolph was first identified as a suspect in the Alabama bombing by the Department of Justice on 14 February 1998, On 5 May 1998, he became the 454th fugitive listed by the FBI on the Ten Most Wanted list. The FBI considered him to be armed and extremely dangerous, and offered a $1 million reward for information leading directly to his arrest. He spent more than five years in the Appalachian wilderness as a fugitive, during which time federal and amateur search teams scoured the area without success. Rudolph was arrested in Murphy, North Carolina, on 31 May 31 2003, by rookie police officer Jeffrey Scott Postell of the Murphy Police Department while Rudolph was looking through a dumpster behind a Save-A-Lot store at about 4 a.m. Postell, while on routine patrol, had initially suspected a burglary in progress. Rudolph was unarmed and did not resist arrest. When arrested, he was clean-shaven with a trimmed mustache, had dyed black hair and wore a camouflage jacket, work clothes, and new sneakers. On 8 April 8 2005, the Department of Justice announced that Rudolph had agreed to a plea bargain under which he would plead guilty to all charges he was accused of in exchange for avoiding the death penalty. The deal was confirmed after the FBI found 250 pounds (110 kg) of dynamite he hid in the forests of North Carolina. His revealing the hiding places of the dynamite was a condition of his plea agreement. The terms of the plea agreement were that Rudolph would be sentenced to four consecutive life terms. Rudolph made it clear in his written statement that the purpose of the bombings was to fight against abortion and the "homosexual agenda." He considered abortion to be murder, the product of a "rotten feast of materialism and self-indulgence." He also believed that its perpetrators deserved death, and that the United States government had lost its legitimacy by sanctioning it. Rudolph considered it essential to resist by force "the concerted effort to

legitimize the practice of homosexuality" in order to protect "the integrity of American society" and "the very existence of our culture", whose foundation is the "family hearth." Eric Rudolph was officially sentenced 18 July 2005, to two consecutive life terms without parole for the 1998 murder of a police officer. He was also sentenced for his various bombings in Atlanta on 22 August 2005, receiving two consecutive life terms. That same day, Rudolph was sent to the Supermax federal prison in Florence, Colorado. His (inmate number 18282-058) and spends 22½ hours per day alone in an 80 square foot concrete cell. In February 2013, with the help from his brother, Rudolph publishes his autobiography, "Between the Lines of Drift: The Memoirs of a Militant." On 11 March 2013, The US Attorney's Office in Birmingham stated in court documents it was seizing Rudolph's royalties from book sales, totaling $200, to pay back the $1 million Rudolph owes in restitution.

SEXTORTION SCAM - WHAT TO DO IF YOU GET THE LATEST PHISHING SPAM DEMANDING BITCOIN: You may have arrived at this post because you received an email from a purported hacker who is demanding payment or else they will send compromising information - such as pictures sexual in nature - to all your friends and family. You're searching for what to do in this frightening situation. Don't panic. Contrary to the claims in your email, you haven't been hacked (or at least, that's not what prompted that email). This is merely a new variation on an old scam which is popularly being called "sextortion." This is a type of online phishing that is targeting people around the world and preying off digital-age fears. We'll talk about a few steps to take to protect yourself, but the first and foremost piece of advice we have: do not pay the ransom. The general gist is that a hacker claims to have compromised your computer and says they will release embarrassing information - such as images of you captured through your web camera or your pornographic browsing history - to your friends, family, and co-workers. The hacker promises to go away if you send them thousands of dollars, usually with bitcoin. What makes the email especially alarming is that, to prove their authenticity, they begin the emails showing you a password you once used or currently use. Again, this still doesn't mean you've been hacked. The scammers in this case likely matched up a database of emails and stolen passwords and sent this scam out to potentially millions of people, hoping that enough of them would be worried enough and pay out that the scam would become profitable. EFF researched some of the bitcoin wallets being used by the scammers. Of the five wallets we looked at only one had received any bitcoin, in total about 0.5 bitcoin or $4,000 at the time of this writing. It's hard to say how much the scammers have received in total at this point since they appear to be using different bitcoin addresses for each attack, but it's clear that at least some people are already falling for this scam. Here are some quick answers to the questions many people ask after receiving these emails.

THEY HAVE MY PASSWORD! HOW DID THEY GET MY PASSWORD? Unfortunately, in the modern age, data breaches are common and massive sets of passwords make their way to the criminal corners of the Internet. Scammers likely obtained such a list for the express purpose of including a kernel of truth in an

otherwise boilerplate mass email. If the password emailed to you is one that you still use, in any context whatsoever, STOP USING IT and change it NOW! And regardless of whether or not you still use that password it's always a good idea to use a password manager. And of course, you should always change your password when you're alerted that your information has been leaked in a breach. You can also use a service like Have I Been Pwned to check whether you have been part of one of the more well-known password dumps.

SHOULD I RESPOND TO THE EMAIL? Absolutely not. With this type of scam, the perpetrator relies on the likelihood that a small number of people will respond out of a batch of potentially millions. Fundamentally this isn't that much different from the old Nigerian prince scam, just with a different hook. By default they expect most people will not even open the email, let alone read it. But once they get a response - and a conversation is initiated - they will likely move into a more advanced stage of the scam. It's better to not respond at all.

SO, I SHOULDN'T PAY THE RANSOM? You should not pay the ransom. If you pay the ransom, you're not only losing money but you're encouraging the scammers to continue phishing other people. If you do pay, then the scammers may also use that as a pressure point to continue to blackmail you, knowing that you're are susceptible.

WHAT SHOULD I DO INSTEAD? As we said before, for sure stop using the password that the scammer used in the phishing email, and consider employing a password manager to keep your passwords strong and unique. Moving forward, you should make sure to enable two-factor authentication whenever that is an option on your online accounts. You can also check out our Surveillance Self-Defense guide for more tips on how to protect your security and privacy online. One other thing to do to protect yourself is apply a cover over your computer's camera. We offer some through our store, but a small strip of electrical tape will do. We know this experience isn't fun, but it's also not the end of the world. Just ignore the scammers' empty threats and practice good password hygiene going forward! See examples of these e-mails at https://www.eff.org/deeplinks/2018/07/sextortion-scam-what-do-if-you-get-latest-phishing-spam-demanding-bitcoin

Operations Security (OPSEC) is everyones responsibility. For more information, contact Roy Lintz, Fort Stewart/HAAF OPSEC Officer at (912) 767-7892.

Fort Stewart and Hunter Army Airfield
http://www.stewart.army.mil/index.php/my-fort/newcomers-1/limit-information

iWATCH, iREPORT, iSalute are community programs to help your neighborhood stay safe from terrorist activities. You and your fellow Army community members can report behaviors and activities that make you feel uncomfortable and do not look right (suspicious behaviors). iWATCH ARMY is a program and partnership between

your community and your local law enforcement. iWATCH ARMY asks you to report behavior and activities that are unusual or seem out of the ordinary. You can submit a report by via phone either by calling your local military police station at Fort Stewart (912) 767-4264 / HAAF (912) 315-6133 and make your report to the MP Desk or if you are in immediate danger or the situation presents an emergency call 911 and submit later report to the MP Desk or your Unit. You can also make a report via the Web at http://www.stewart.army.mil/ info/?id=541&p=2. **Do not try to investigate on your own**, report incident to law enforcement.

Ten Most Wanted - http://www.fbi.gov/wanted/topten
Most Wanted Terrorists - http://www.fbi.gov/wanted/wanted_terrorists
Seeking Terror Information - http://www.fbi.gov/wanted/terrorinfo
Crime Alerts - http://www.fbi.gov/wanted/alert
Kidnappings & Missing Persons - http://www.fbi.gov/wanted/kidnap
Fugitives and Missing Persons - http://www.fbi.gov/wanted
Rewards For Justice - http://www.rewardsforjustice.net/
Interpol - http://www.interpol.int/en
Centers for Disease Control and Prevention - https://www.cdc.gov/
Active U.S. Hate Groups Map - http://www.splcenter.org/hate-map
ADL Hate Symbols Database - https://www.adl.org/education-and-resources/resource-knowledge-base/hate-symbols
National Gang Center - http://www.nationalgangcenter.gov/
World's Immigration Map - http://metrocosm.com/global-immigration-map/
Drug and Pill Identifier Tool - https://www.drugs.com/imprints.php
Savannah Police Weekly Top 10 Most Wanted - http://savannahpd.org/mostwanted/

In accordance with Title 17 <U.S.C.> Section 107, this material is distributed without profit or payment to those who have expressed a prior interest in receiving this information for educational purposes only. Fort Stewart Weekly Report is provided free as a security education product by the Fort Stewart DPTMS, Security Division, Fort Stewart, GA.

Suggestions Your comments are very important. If you have any recommendations or comments (good or bad) concerning this product, please direct them to LeRoy Malphrus, Chief, Security Division, Fort Stewart, GA; COM Tel: (912) 767-1910/1891; FAX: 767-2994; e-mail**:** leroy.h.malphrus.civ@mail.mil.